BOIES SCHILLER FLEXNER LLP
David Boies (admitted pro hac vice)
333 Main Street
Armonk, NY 10504
Tel.: (914) 749-8200
dboies@bsfllp.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsfllp.com
brichardson@bsfllp.com

James Lee (admitted pro hac vice)
Rossana Baeza (admitted pro hac vice)
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsfllp.com
rbaeza@bsfllp.com

Alison L. Anderson, CA Bar No. 275334
M. Logan Wright, CA Bar No. 349004
2029 Century Park East, Suite 1520
Los Angeles, CA 90067
Tel.: (213) 995-5720
alanderson@bsfllp.com
mwright@bsfllp.com

SUSMAN GODFREY L.L.P.
Bill Carmody (admitted pro hac vice)
Shawn J. Rabin (admitted pro hac vice)
Steven M. Shepard (admitted pro hac vice)
Alexander Frawley (admitted pro hac vice)
Ryan Sila (admitted pro hac vice)
One Manhattan West, 50th Floor
New York, NY 10001
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@susmangodfrey.com
rsila@susmangodfrey.com

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel.: (310) 789-3100
abonn@susmangodfrey.com

MORGAN & MORGAN
John A. Yanchunis (admitted pro hac vice)
Ryan J. McGee (admitted pro hac vice)
Michael F. Ram, CA Bar No. 104805
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com
mram@forthepeople.com

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No.: 3:20-cv-04688-RS

PLAINTIFFS' OPPOSITION TO GOOGLE'S MOTION FOR SUMMARY JUDGMENT

The Honorable Richard Seeborg
Courtroom 3 – 17th Floor
Date: July 25, 2024
Time: 1:30 P.M.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

Google's motion raises three central issues, all of which are disputed: (1) whether Google accurately represents what its simple on/off (s)WAA button does; (2) whether the (s)WAA-off app activity data Google collects and saves is identifying; and (3) whether Google harms users and profits from its collection and use of their (s)WAA-off data. Every argument Google makes is contradicted by ample evidence and authorities that Google simply ignores. Because a reasonable juror could readily find in Plaintiffs' favor on all claims, summary judgment should be denied.

Evidence Google Does Not Address. Evidence supporting Plaintiffs includes not only their testimony but also documents and testimony from Google employees, opinions offered by both sides' experts, and user studies Google itself commissioned. For example, Google employees acknowledged the at-issue disclosures are "intentionally vague" regarding the effect of (s)WAA and the existence of data "collected outside of the[] Google Account" (Mao Ex. 1 at -02), complained that Google's disclosures are a "real problem" and do not "accurately describe what happens when WAA is off" (Ex. 2 at -11), and conducted a user study which found that ***"[a]ll participants*** expected turning WAA toggle off to stop saving their activity" (Ex. 3 at -00, -11). Even Google CEO Sundar Pichai inaccurately testified to Congress that Google's users "can clearly see ***what information we have***—we actually show it back to them. We give clear toggles, by category, where they can decide ***whether that information is collected, stored ….***" Ex. 4 (Hochman Rep.) ¶ 256. The record also includes expert and documentary evidence that Google saves sensitive (s)WAA-off data with unique identifiers, many of which *Google creates, manages, and uses* to identify class members. Hochman Rep. ¶¶ 100-10. Google exploits (s)WAA-off data for its own benefit, to improve Google products and generate advertising profits, including from conversions. Ex. 5 at 16, 20, 22, 28; Ex. 6 at 209:8-210:5; Hochman Rep. § VII.F.

Authorities Google Does Not Address. Google also fails to address relevant law, including cases decided against Google on these same issues. Google does not even cite the recent summary judgment decision in *Brown v. Google LLC*, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023), which soundly rejected arguments that are the same or similar to those Google asserts here. Other examples abound. In *Opperman v. Path, Inc.*, the court denied summary judgment on the issue of consent where the disclosures did not "explicitly address" the challenged conduct. 205 F. Supp. 3d 1064, 1074 (N.D. Cal. 2016). In *In re Google RTB Consumer Priv. Litig.*, the court recognized that "unique device identifiers" are "personal information" and identifying under California law and Google's Privacy Policy. 606 F. Supp. 3d 935, 944 (N.D. Cal. 2022). In *Campbell v. Facebook, Inc.*, the Ninth Circuit held that surreptitious monitoring of online activity gave rise to a legally cognizable privacy harm. 951 F.3d 1106, 1117 (9th Cir. 2020). In *In re Carrier IQ, Inc.*, the court rejected the argument, advanced by Google here, that battery depletion and slower performance does not qualify as "damage or loss" under the CDAFA. 78 F. Supp. 3d 1051, 1066-67 (N.D. Cal. 2015); *see also Williams v. Facebook, Inc.*, 498 F. Supp. 3d 1189, 1200 (N.D. Cal. 2019) (Seeborg, J.). All of these cases have been cited to or by this Court in this case.

Rulings in this Case Google Does Not Address. Google also ignores how its arguments contradict this Court's holdings in prior stages. In its motion to dismiss ruling, for example, this Court *rejected* Google's argument that that the very same disclosures established consent. Instead, Plaintiffs offered "a cogent account of why they saw [(s)]WAA as capable of turning off GA for Firebase's collection of their third-party app data." Dkt. 109 at 10. Similarly, the Court recognized at class certification that "damage or loss" under the CDAFA can be shown without "a corresponding loss, as 'California law recognizes a right to disgorgement of profits resulting from unjust enrichment.'" Dkt. 352 at 11 (quoting *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 599-600 (9th Cir. 2020)). Google cannot win summary judgment by repackaging the same arguments this Court already rejected. *See Am. Canoe Ass'n v. D.C. Water & Sewer Auth.*, 306 F. Supp. 2d 30, 34 (D.D.C. 2004) ("[A] summary judgment motion 'may not be made on the same grounds and with the same showing that led to the denial of a previous motion to dismiss.'" (quoting Wright & Miller, Fed. Prac. & Proc. § 2713)). Google's prayer for a do-over is particularly misplaced given the extensive evidence uncovered in discovery supporting Plaintiffs.

II. TRIABLE MATERIAL FACTS

A. Plaintiffs Dispute Google's "Undisputed Facts"

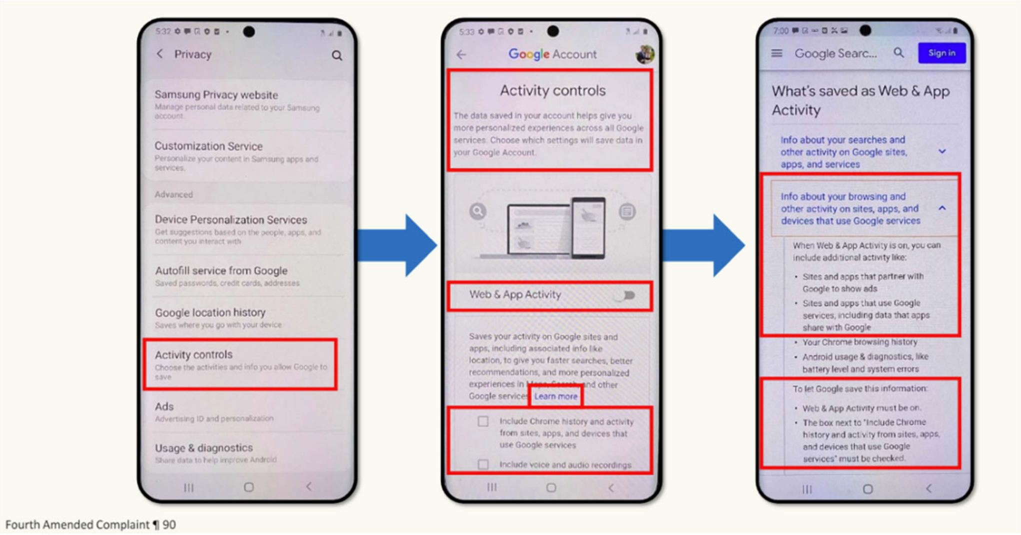
Google asserts eight purportedly "undisputed facts." Mot. at 16-17. They are disputed, as summarized in this chart and explained in more detail throughout this brief.

Google's "Undisputed Facts"	**Plaintiffs' Response**
Fact 1: "The WAA button controlled whether certain data would be 'saved to your Google Account.'" Mot. at 16.	Disputed. Plaintiffs dispute Google's self-serving interpretation of its disclosures. Plaintiffs, multiple Google employees, and all of the respondents in a 2020 Google user study interpreted the at-issue Google disclosures to stop Google from collecting and saving app activity data when (s)WAA was turned off, an interpretation that is also supported by the lengthy report of Plaintiffs' privacy expert. *See infra* § IV.A. Plaintiffs' interpretation is consistent with Google's representation that (s)WAA "must be on" to "let Google save" app activity data. Ex. 7. Plaintiffs' interpretation is also consistent with and supported by the Privacy Policy, which links to the (s)WAA controls and states that users "can adjust your privacy settings to control what we collect *and* how your information is used." Ex. 8 at 1; Exs. 9-25.[1]
Fact 2: "The phrase 'saved to your Google Account' limited the ambit of the WAA button to permissions relating to saving data in a manner that was associated with personal information." *Id.* at 16-17.	
Fact 3: "Google represented through its Privacy Policy and Privacy Portal that the phrase 'saved to your Google Account' meant "associated with your personal information.'" *Id.* at 17.	Disputed. No Google disclosure states this. The Privacy Policy does not even define "Google Account," as Google's disclosures expert conceded. Ex. 8; Ex. 32 at 294:22-296:14. Google employees admit that Google's disclosures are "intentionally vague" about data "saved outside of the[] Google Account." Ex. 1. A juror could find that reasonable person would believe the Google Account comprises all data Google collects about your activity, or at least all data with identifiers *Google creates and manages*.
Fact 5: "Google did not save the WAA-off or (s)WAA-off data at issue in this case generated by class members to that class member's Google Account." *Id.*	Disputed. Through discovery, Plaintiffs obtained evidence establishing that Google saves identifying information when (s)WAA is off, including Google identifiers that pinpoint a specific person's phone. Hochman Rep. ¶¶ 100-10, 202, 220-28, 248, 301. Google was able to identify Plaintiffs' (s)WAA-off activity with just their Google identifiers. Hochman Rep. ¶¶ 176, 178-79. Google's internal documentation also
Fact 6: "Google did not associate the WAA-off or (s)WAA-off data at issue in this case generated by class members with the class members' personal information." *Id.*	
Fact 4: "Personal information" meant information "which personally identifies you	

[1] Earlier versions of the Privacy Policy likewise represented that "Google activity controls" allows users to "decide what types of data . . . you would like saved with your account when you use Google services." Ex. 26 at 5; Ex. 27-31 (same).

. . . which can be reasonably linked to such information by Google, such as information we associate with your Google account." *Id.*	confirms that the device and application-based identifiers at issue in this case cannot "be blocked from joining PII [personally identifying information]." Ex. 33 at -41. Google's employees admit that Google can "link app events collected by [Firebase] to [Google Account] ID even if end users turn off WAA." Ex. 34. Moreover, (s)WAA-off data qualifies as "personal information" even under Google's asserted definition, including because the data can be "reasonably linked" to the "Google Account" identifier.
Fact 7: "Google maintained the WAA-off or (s)WAA-off data at issue in this case generated by class members in pseudonymous or anonymous form in a manner that disabled Google employees from personally identifying the user that generated the data." *Id.*	
Fact 8: "Google never used the WAA-off or (s)WAA-off data at issue in this case generated by class members to personalize advertising to class members or build marketing profiles." *Id.*	<u>Disputed</u>. Google uses (s)WAA-off data to target advertisements based on criteria such as location, expressed interest (inferred from the open app), and language. Hochman Rep. ¶¶ 273-77. Google also creates comprehensive profiles of (s)WAA-off users' app activity that it uses for advertising purposes, such as conversion tracking, which is lucrative for Google. *Id.* ¶¶ 279-82. Google exploits (s)WAA-off data for other purposes, too. *See* Ex. 6 at 209:8-210:5 ((s)WAA-off data "is logged for product improvement purposes"); Ex. 35 at 207:8-10 (Google's AI uses (s)WAA-off data).

B. The Relevant Disclosures



Privacy

Samsung Privacy website
Manage personal data related to your Samsung account.

Customization Service
Personalize your content in Samsung apps and services.

Advanced

Device Personalization Services
Get suggestions based on the people, apps, and content you interact with

Autofill service from Google
Saved passwords, credit cards, addresses

Google location history
Saves where you go with your device

Activity controls
Choose the activities and info you allow Google to save

Ads
Advertising ID and personalization

Usage & diagnostics
Share data to help improve Android

Google Account

Activity controls

The data saved in your account helps give you more personalized experiences across all Google services. Choose which settings will save data in your Google Account.

Web & App Activity

Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services. Learn more

□ Include Chrome history and activity from sites, apps, and devices that use Google services

□ Include voice and audio recordings

Google Searc... Sign in

What's saved as Web & App Activity

Info about your searches and other activity on Google sites, apps, and services

Info about your browsing and other activity on sites, apps, and devices that use Google services

When Web & App Activity is on, you can include additional activity like:

- Sites and apps that partner with Google to show ads
- Sites and apps that use Google services, including data that apps share with Google
- Your Chrome browsing history
- Android usage & diagnostics, like battery level and system errors

To let Google save this information:

- Web & App Activity must be on.
- The box next to "Include Chrome history and activity from sites, apps, and devices that use Google services" must be checked.

Fourth Amended Complaint ¶ 90

Ex. 36 (enlarged version). A juror could easily agree with Plaintiffs' interpretation of Google's disclosures. As shown above, Google directs users to the (s)WAA toggles with representations that users can control what data Google collects and saves—not merely where or how Google saves it. On Android, the Privacy menu says users can "[c]hoose the activities and info you allow Google to save." Ex. 36 (Screen 1).[2] This option directs users to Google's "Activity Controls" page, which includes the (s)WAA toggles. *Id.* (Screen 2). Google's Privacy Policy likewise assures users that "you can adjust your privacy settings to ***control what we collect*** and how your information is used." Exs. 8 at 1, 9-25.[3] The Privacy Policy also represents that "[t]he ***information Google collects***, and how that information is used, depends on how you use our services and how you manage your privacy controls." *Id.* at 2.[4] With a hyperlink, the Privacy Policy directs users to "privacy controls" on the Activity Controls page, including (s)WAA. *Id.* at 7-8.

On Google's Activity Controls page, which is the same for all class members (Android and non-Android), Google explains that (s)WAA "[s]aves your activity on . . . sites and apps that use Google services." Ex. 39 (Screen 2); Ex. 40 at -90-91. This Google page also invites users to "Learn more" on the hyperlinked Google "WAA Help Page," where Google represents that (s)WAA "***must be on***" to "***let Google save***" activity on "apps that use Google services, ***including data that apps share with Google***." Ex. 36 (Screen 3); Ex. 7 (materially identical versions of this page).[5] Based on these uniform Google disclosures, a reasonable juror could easily find that Google promised it would not collect or save (s)WAA-off app data. *See infra*, § IV.A.

Volumes of evidence support Plaintiffs' interpretation. In April 2020, a Google user study found that "***[a]ll participants expected turning WAA toggle off to stop saving their activity***." Ex. 3. Months later, in connection with another user study, Google's researcher Arne de Booij predicted that "***[m]ost respondents*** will believe that ***turning off WAA*** will result in ***no data being collected*** from their activity ***and no personalisation*** in Google products and services." Ex. 41 at -99. He correctly identified collection and personalization as separate issues, and he predicted—

[2] *See* Ex. 37 at 3 (Google confirming that Screen 1 did not change during the class period).

[3] *See supra* note 1, regarding earlier Privacy Policies.

[4] The webpage that Google cites in footnote 17 on page 12 supports Plaintiffs; it reinforces that users "can control the information collected by Google on these sites and apps." Ex. 38 at -56.

[5] The Privacy Policy defines "Google services" to include "[p]roducts that are integrated into third-party apps and sites, like ads [and] analytics." Ex. 8 at 1; Exs. 9-25. Earlier versions of the Privacy Policy similarly defined Google's "services" to include "services offered on other sites (such as our advertising services)." Ex. 26 at 8; Exs. 27-31 (same).

months before this lawsuit—that people expect ***neither***. *See also infra* § IV.A (further evidence).

Disagreeing with its own employees, Google now offers a much different interpretation of the disclosures. Google argues that the only reasonable interpretation of these disclosures is that the user has *no* power to stop Google from collecting and using app activity data, and that the *only* thing the (s)WAA toggle does is cause all that data not to be "associated with personal information." Mot. at 16-18.[6] Google constructs this interpretation from two disclosures that refer to data "saved to your Google Account if [(s)WAA] is turned on." Ex. 7 at -22. From there, Google makes the dubious leap that the "limited ambit of" of (s)WAA is "obvious" because "to your Google Account" means "associated with your personal information." Mot. at 2, 11. Google even goes so far as to call "Google Account" a "defined term." Mot. at 11. There is no such definition. Google's Privacy Policy states:

> **Google Account:** You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address, and a password). This account information is used to authenticate you when you access Google Services and protect your account from unauthorized access by others. You can edit or delete your account at any time through your Google Account settings.

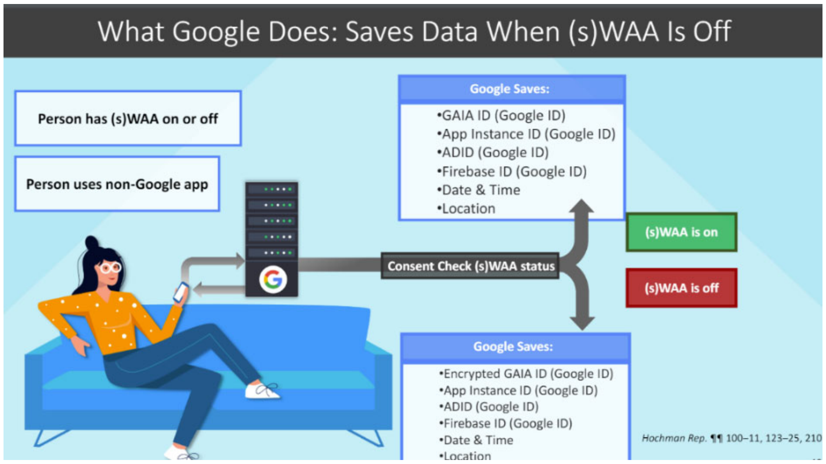
Ex. 42 at 22-23. The text says precisely nothing about what information is and is not considered part of the "Google Account." All this remains, as this Court previously put it, "at best, nebulous." Dkt. 109 at 8. Google fails to explain why a juror could not reasonably find that users would instead interpret these disclosures as stating that their Google Accounts would include all data associated with Google's own identifiers, such as device and application IDs. Interpreting these disclosures is an issue for the jury.

C. Google's Collection and Saving of (s)WAA-Off Data.

Google's contention that "[t]here is no dispute" that (s)WAA-off data "cannot be joined with any person" (Mot. at 20) is both false and beside the point. Plaintiffs obtained ample evidence establishing that Google collects and saves identifying information when (s)WAA is off. *See* Ex. 43 at 160:21-161:8 (Plaintiffs' expert testifying that Firebase events "send identifiers that are linked to an individual"). Indeed, Google saves this app activity data alongside each user's digital

[6] Plaintiffs dispute that (s)WAA-off data is not associated with personal information. *Infra*, § II.C.

fingerprint. For example, Google collects information that uniquely identifies the user's personal mobile device, most commonly ADID (a Google-created identifier on Android) and IDFA (on iOS). Hochman Rep. ¶¶ 102-04. Google also collects Google-created identifiers that uniquely identify an app installation on a specific user's device, such as Google's own app_instance_id and Firebase instance ID. *Id.* ¶ 315. Google's SDKs also automatically collect the user's IP address, age, gender, geolocation (*Id.* ¶¶ 89, 93, 99, 105, 129, 223), as well as identifiers tied to the user's log-in credentials with non-Google apps (*Id.* ¶ 326), and dozens of other identifiers (*Id.* ¶ 110). Google mentions *none* of this as it attempts to present its interpretation as an "undisputed fact." Indeed, Google flat-out ignores just how similar the data it collects while (s)WAA is off to the data it collects while (s)WAA is on.



What Google Does: Saves Data When (s)WAA Is Off

Person has (s)WAA on or off

Person uses non-Google app

Google Saves:
•GAIA ID (Google ID)
•App Instance ID (Google ID)
•ADID (Google ID)
•Firebase ID (Google ID)
•Date & Time
•Location

Consent Check (s)WAA status

(s)WAA is on

(s)WAA is off

Google Saves:
•Encrypted GAIA ID (Google ID)
•App Instance ID (Google ID)
•ADID (Google ID)
•Firebase ID (Google ID)
•Date & Time
•Location

Hochman Rep. ¶¶ 100–11, 123–25, 210

Google regularly uses its identifiers to, well, *identify* its users, *even when (s)WAA is off.* When (s)WAA is off, *Google matches the user's device identifier with their GAIA ID*, and Google contends that the GAIA ID is the sum and substance of a Google Account. Hochman Rep ¶¶ 165, 305, 307; Ex. 5 at 18 (Google "check[s] for user consent" using "DSID/IDFA"). As Plaintiffs' technical expert opines, Google's distinction between GAIA and non-GAIA identifiers is also a "false dichotomy." Ex. 43 at 53:18-54:2. Other identifiers, including device-based identifiers, are equally identifying. For example, when Google serves interest-based ads to a (s)WAA-*on* user, it infers *that user's* interests from activity tied to their device identifier. *See* Ex. 44 at -08.R ("remarketing lists" "use Device ID (IDFA/ADID) to . . . identify the target"); Ex. 45 at -66. Google tracks *each specific user* by device identifier to measure the impact of Google's ads.

Hochman Rep. ¶¶ 279-82, 309-10. In this case, Google even used the same identifiers to reproduce voluminous amounts of Plaintiffs' data in discovery. *Id.* ¶¶ 178-80. Google again fails to mention any of this evidence or its tacit admissions.

Google also fails to grapple with evidence that its allegedly "pseudonymous" data is anything but pseudonymous. Google's internal documentation confirms that the device-based and application-based Google identifiers at issue here "*[c]an[not] be blocked* from joining PII [personally identifying information]." Ex. 33 at -341. Employees recognized that Google could "retrieve" purportedly "pseudonymous" data like ADID and app_instance_id if given a "GAIA ID *for users turning off WAA*," for example in response to a "[s]ubpoena." Ex. 34 (discussing "ability to link app events … to GAIA ID even if end users turn off WAA"). Former Google engineer Blake Lemoine, a Google AI engineer-turned-whistleblower, testified under oath that Google's AI-powered systems use "WAA-off data" and combine it with users' WAA-on identity. *See* Ex. 35 at 205:25-207:9. Plaintiffs' technical expert also explained at length how (s)WAA-off data is identifying and "linked to users." Hochman Rep. § VII.G.

Google also ignores evidence that the at-issue data reveals a startling amount of information about class members' personal lives. The average person spends four hours a day on mobile apps. Hochman Rep. ¶ 1. Most popular apps are embedded with Google's Firebase and GMA SDKs. In 2020, Google's Firebase SDK was embedded in 97% of the top 1,000 apps on Android and 54% on iOS. Ex. 46 at -729; *see also* Hochman Rep. ¶ 2 (Google's GMA SDK embedded in approximately 80% of apps). Google uses these SDKs to learn each app that a user installs and opens, each screen they visit, each video they watch, each bit of content they select, each purchase they make, the amount of time they spend on each app and screen, and more. *See* Hochman Rep. ¶ 98. Bruce Schneier, a renowned expert on privacy and security, explains that what users do on apps reveals highly personal information regarding those individuals:

> It may reflect, for example . . . political and religious beliefs, [s]exual orientation and proclivities, their reproductive cycle and intentions, their medical history and diagnoses, their weight and dietary preferences, their plans to find new employment or move to another location, their experience of domestic abuse, or other . . . personal circumstances.

Ex. 47 (Schneier Rep.) ¶ 89; *see also* Hochman Rep. ¶ 188 (data revealing gastrointestinal issues).

Google euphemistically calls its conduct "record-keeping," but these Google records are sensitive information about class members that Google collected and saved with (s)WAA turned off.

D. Google's Use and Monetization of (s)WAA-Off Data.

Google is not a mere "service provider" working as an agent for app developers. Mot. at 7, 25. Google uses (s)WAA-off app activity data for its own independent benefit, including to target ads, to track conversions, to convince advertisers to pay Google more than Google pays to purchase ad space from app developers, and to further develop Google products.

Plaintiffs' expert describes how Google uses (s)WAA-off data to target or personalize ads based on criteria such as location, expressed interest (inferred from the open app), and language. Hochman Rep. ¶¶ 273-77. Google also builds comprehensive accounts of class members' (s)WAA-off app activity, which Google uses to track and attribute advertising conversions, which are valuable events such as purchases and downloads. *Id.* ¶¶ 92, 234. When a conversion occurs, Google consults data from the apps that the particular user visited, the ads they saw, and when this activity occurred. *Id.* ¶¶ 279-82. Google then decides whether to claim that a Google-served ad deserves credit for the conversion, which is called "attribution." *Id.* ¶¶ 279-82. Google claims that this process—where Google creates a comprehensive profile of class members' app activity, which is used for advertising purposes—does not qualify as a "marketing profile" (Mot. at 17) and is mere "basic record-keeping" (Mot. at 7-8), a term apparently manufactured by counsel during class certification, because this reference to "basic record-keeping" appears nowhere in the disclosures Google cites. Only the jury can decide whether to accept Google's dubious characterization.

It is also false for Google to claim that it collects and processes (s)WAA-off data exclusively to provide analytics services for the benefit of app developers. *See* Mot. at 25 (claiming Google is only developers' "vendor" or "agent"). Google's ad business uses (s)WAA-off data to implement a profitable arbitrage strategy. First, Google buys ad space from app developers at a fixed price that Google must pay. *See* Ex. 48 at 3 (Google "always pay[s] publishers for their ad space"). Then Google sells that space to advertisers. But "the vast majority [of Google's] advertisers only pay when a user takes an action after seeing their ad." *Id.* at 3. Google's ability to monitor and take credit for user app activity makes a massive difference between advertising profits and losses. *See id.* at 3 (Google "tak[es] on the risk of showing ads to users"); Ex. 49 at -72-75 (estimating revenue loss from inability to track conversions in related context); Hochman Rep. ¶ 280. Google's profits from users' (s)WAA-off data are substantial. Plaintiffs' damages expert, Michael Lasinski, calculated that through 2022, Google's ads business profited at least **$664.3 million** from using (s)WAA-off app activity data. Ex. 50 (Lasinski Rep.) ¶ 129 & fig.43. Of that, **$558.8 million** was from attributing conversions. *Id.* ¶ 112 & fig.34.

Regardless of whether the data is "identifying" (which is not what the law requires), Google uses (s)WAA-off app activity data to extract still more value by using it. Google admits that it uses the data at issue to improve its products and services. *See* Hochman Rep. § VII.G.3; Ex. 5 at 16, 28 (Google "uses data collected via GA for Firebase across teams for product development, improvement, and diagnostics"); Ex. 6 at 209:8-210:5 ((s)WAA-off data "is logged for product improvement purposes"). Google's AI also ingests (s)WAA-off data. Ex. 35 at 207:8-10. According to Google, there are so many "downstream users" of (s)WAA-off data by Google that it was "not practical" for Google to identify every implicated data repository. Ex. 51 at 4.

III. LEGAL STANDARD

"The court must draw all reasonable inferences in favor of [Plaintiffs], including questions of credibility and of the weight to be accorded particular evidence." *Nat'l Fire Ins. v. Fed. Ins.*, 843 F. Supp. 2d 1011, 1014 (N.D. Cal. 2012) (Seeborg, J.). Summary judgment may be granted only if "the record taken as a whole could not lead a rational trier of fact to find for the non-moving party." *Matsushita Elec. Indus. Co. v. Zenith Radio*, 475 U.S. 574, 587 (1986). The Supreme Court counsels "caution in granting summary judgment." *Consumer Fin. Prot. Bureau v. Nationwide Biweekly Admin., Inc.*, 2017 WL 11673197, at *2 (N.D. Cal. Feb. 6, 2017) (Seeborg, J.).

IV. ARGUMENT

A. A Reasonable Juror Could Find There Was No Consent.

To win on consent, Google must prove that its disclosures "are unambiguous" and "not susceptible to Plaintiffs' reading." Mot. at 18; *Brown v. Google*, 2023 WL 5029899, at *8 (N.D. Cal. Aug. 7, 2023) (denying summary judgment because Google's disclosures were not "unambiguous[]").[7] The required showing of "[e]xpress consent . . . is 'consent that is clearly and unmistakably stated.'" *Satterfield v. Simon & Schuster*, 569 F.3d 946, 955 (9th Cir. 2009). Moreover, consent is effective only if it is "voluntary." *Hill v. NCAA*, 7 Cal. 4th 1, 26, 43 (1994).

Summary judgment is unwarranted because a reasonable juror could find there was no consent for the challenged Google conduct. *See Opperman*, 205 F. Supp. 3d at 1074 (denying summary judgment based on consent where the disclosures did not "explicitly address" the challenged conduct); *see also Digital Envoy, Inc. v. Google, Inc.*, 370 F. Supp. 2d 1025, 1033 (N.D. Cal. 2005) (Seeborg, J.) (denying summary judgment where language was "susceptible to more than one reasonable interpretation," which means "Google has failed to establish that it is entitled to judgment as a matter of law"). Google's consent arguments rely on the same disclosures presented in support of Google's motion to dismiss (*see* Dkt. 62 at 7). Google never explains why this Court should now find that they unambiguously permit the at-issue Google conduct (which goes far beyond "record keeping"), especially given the substantial evidence uncovered in discovery that supports Plaintiffs' claims.

1. The Evidence Makes Clear There is a Material Dispute Over Consent.

A reasonable juror could readily agree with Plaintiffs that Google represented that it would not collect or save app activity when (s)WAA was off. *Supra* § II.A. Google represented that users can "choose the info and activities you allow Google to save," and nowhere stated that (s)WAA merely controls *where* or *in what form* Google saves that data. Ex. 36 (Screen 1); *see also* Ex. 8 at 1 (Privacy Policy, "control what we collect"). Google also explained that (s)WAA "must be on" to "let Google save" activity on "sites and apps that use Google services." *See* Ex. 7. Every Plaintiff interpreted the Google disclosures to mean that Google would not collect or save their app activity data when (s)WAA was off. *See* Ex. 52 at 143:19-145:17 (testimony by Santiago); Ex. 53 at 132:3-134:4 (Cataldo); Ex. 54 at 81:18-83:22 (Harvey); Ex. 55 at 94:18-98:5 (Rodriguez). Indeed, Google itself refers to (s)WAA as a "consent" signal, and internal documents describe (s)WAA-off data as "unconsented." *See* Ex. 56 at -43; Hochman Rep. ¶¶ 161, 166, 175.

[7] The CDAFA invokes "permission," not consent. *See* Cal. Penal Code § 502(c)(2). Because Google's motion asserts that users expressly consented, Plaintiffs treat the two issues together.

Documents produced by Google support Plaintiffs' reading. In July 2019, Google engineer Chris Ruemmler assessed the same Google disclosures and wrote that "***we don't accurately describe what happens when WAA is off***." Ex. 2 at -10. As he understood the disclosures, they represented that when (s)WAA is off, "Google does ***not*** save information like . . . ***ads you click, or things you buy on an advertiser's site***." *Id.* (emphasis added). Mr. Ruemmler confirmed during his deposition that he interpreted "off" to mean off—that such data would not be sent to Google, Ex. 57 at 72:21-73:3, which tracks Plaintiffs' understanding of the same disclosures. Without identifying examples, Google accuses Plaintiffs of "grossly misus[ing] internal emails" at class certification. Mot. at 19. Google claims that employees' "concerns" about (s)WAA are "unrelated" to this case, and that these employees at deposition denied "shar[ing] Plaintiffs' extreme reading of WAA." *Id.* at 20. The record does not support Google's assertion. For example, Mr. Ruemmler at deposition agreed that Google's (s)WAA disclosures should be rewritten to specifically address how Google saves (s)WAA-off data outside of the "Google Account":

> Q. You thought at the time that Google needed to ***modify the help article to address what happens with WAA with respect to data that's not tied to someone's account***?
>
> A. That was a suggestion I made.

Ex. 57 at 90:4-8 (emphasis added); *see also* Ex. 2 at -11 (Mr. Ruemmler writing in July 2019 that "We still would need to modify the help article above to indicate that WAA off is identical to being not logged into your account (data logged, but not tied to your account)"). Mr. Ruemmler persisted, writing in December 2019 that "***Isn't WAA off supposed to NOT log at all? At least that is what is implied from the WAA page***. So, if WAA is off, how are we able to log at all?" Ex. 58 at -81 (emphasis added). In August 2020, shortly after this case was filed, he wrote that WAA is "completely broken" because there is "no way for the user to determine what this actually controls." Ex. 59 at -46. Many other Google employees expressed similar concerns:

- In 2017, an internal Google presentation referred to WAA and sWAA as ***"losers"*** because people "didn't understand the sWAA text." Ex. 60 at -66.
- In 2018, Google employee J.K. Kearns wrote *"**teams should not use user data at all if WAA is off**"* which is what "most users expect." Ex. 61 at -14.
- In 2019, Google employee Brenda Chen wrote "this is an ongoing struggle that ***people don't understand what Web and App Activity is***." Ex. 62 at -64.

- In March 2020, another employee wrote "The reality is so complex with WAA that ***not even *we* understand exactly what happens***." Ex. 63 at -12.
- In June 2020, Google user experience researcher Arne de Booij predicted that ***users "will believe that turning off WAA will result in no data being collected from their activity***." Ex. 41 at -99.R.
- In July 2020, Mr. Kearns wrote in an internal email that "to me, it feels like a fairly significant bug that ***a user can choose to turn off WAA but then we still collect and use the data*** (even locally)." Ex. 64 at -82.R.
- In August 2020, another employee complained that Google's "language" about WAA "feels vague and hard-to-parse for non-engineers / lawyers." Ex. 65 at -680.

In user studies, Google also confirmed that people share Plaintiffs' expectations. In April 2020, one Google study found that "***<u>all</u> participants expected turning WAA toggle off to stop saving their activity***." Ex. 3 at -00, -11 (emphasis added). Other studies had similar results:

- A 2017 Google presentation summarized a user research study, explaining that the "effect of the activation of the Web & App Activity is *not well understood*," and recommending "simple language" to describe it. Ex. 66 at -706.
- A 2019 Google presentation summarized "Data Retention Usability Study Findings," and flagged "persistent points of confusion," including "uncertainty about what type of data is impacted by controls" and that "WAA is not clear to users." Ex. 67 at -82.
- A spreadsheet summarizing "Key Insights" from a user experience research study stated that "WAA settings are hard to understand." Ex. 68.
- In another study, an employee wrote: "WAA just isn't clear to users." Ex. 69 at -239.

To the extent Google argues any of the above evidence did not exclusively address app activity data, that is irrelevant. The (s)WAA toggles and disclosures expressly apply to different types of data, including app activity data, and the accuracy of these disclosures as applied to any listed type of data bears on their accuracy as applied to app activity data. Regardless, the jury must weigh the evidence and decide whether it supports Plaintiffs' or Google's interpretation.

That evidence includes the sworn Congressional testimony of Google CEO Sundar Pichai. Pichai testified that Google "give[s] clear toggles, by category, where [users] can decide ***whether*** that information is collected [and] stored." Hochman Rep. ¶ 256. Mr. Pichai represented one thing ("clear toggles" controlling "whether" data is collected), but Google implemented a system that still collects and stores data when that "toggle" is off. Google now contravenes its own CEO and claims there is no "account control to disable Google's collection." Mot. at 12. If Mr. Pichai cannot understand (or accurately describe) the disclosures, where does that leave ordinary users?

Finally, Google mischaracterizes Plaintiffs to be asserting that (s)WAA promised only to be an "ad blocker." Mot. at 13. This is nonsense—Plaintiffs instead allege the (s)WAA toggle promises something quite different: Google will not save or use (s)WAA-off data at all, whether for ads or not. As Plaintiff Cataldo testified, "the ad setting doesn't override and now allow Google to collect information that I didn't allow it to collect in the first place." Ex. 53 at 153:2-8.

2. Evidence Undermines Any "Google Account" Argument.

Google's focus on "Google Account" once again fails to provide any basis for judgment in Google's favor. The Court correctly rejected this same argument on Google's motion to dismiss. *See* Dkt. 62 at 7 (Google arguing the "disclosures are about what Google stores in users' Google Accounts"). Reviewing the disclosures, the Court reasoned that "the concept of a 'Google Account' is, at best, nebulous," failing to provide "a succinct plain English explanation of what exactly a Google Account is." Dkt. 109 at 8-9 The Court found the same when granting certification. *See* Dkt. 352 at 14-15. The only new thing is that discovery has unearthed substantial evidence supporting Plaintiffs' interpretation of these same disclosures. Google has no basis to rehash arguments this Court has already rejected. *See Am. Canoe Ass'n*, 306 F. Supp. 2d at 34-35.

Here is how Google actually presents "Google Account" in its Privacy Policy: "You may access some of our services by signing up for a Google Account and providing us with some personal information (typically your name, email address, and a password)." Ex. 42 at 22-23. Even Google's own disclosures expert agreed that this is not a *definition* of the term "Google Account". Ex. 32 at 295:22-296:14 (admitting "there is no header [with] the definition of 'Google account.'"). It certainly does not demonstrate for the purposes of summary judgment that Google disclosed to users that the company collects and saves data *in* other places that Google does not consider to be their "Google Accounts," or that information associated with Google identifiers can be stored by Google outside of the "Google Account."

Google argues that "saved to your Google Account" means "<u>associated with your personal information</u>" (Mot. at 11), but no Google disclosure actually says that. Google took this phrase from a portion of its Privacy Policy that does not even mention "Google Account":

> We may combine the information we collect among our services and across your devices

> for the purposes described above . . . [I]f you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered . . .%

Ex. 8 at 7. Google cannot show the absence of a genuine issue of material fact on the back of its made-for-litigation "definition" of "Google Account." But even if a (s)WAA-off user were to squint sideways at this portion of the policy and see in it Google's desired limitation of the term "Google Account" to mean *only* data "associated with" that user's "personal information" (and there is no evidence that any consumer had this perspective) that still would not justify summary judgment. That same user would reasonably believe that the activity data Google collected, stored, and linked to unique, personal identifiers, was part of that user's Google Account. Google's strained argument confounds a reference to possibility for exclusivity.

Google then relies on a statement in its Privacy Policy that "[w]hen information is associated with your Google Account, we treat it as personal information." Mot. at 11. This does not explain what data is associated with a "Google Account," and it certainly does not disclose that there are *other* repositories where Google saves data about account holders' activity with those account holders' identifiers, including data collected when users had turned off (s)WAA.

Google also refers to a distinction between "personal information" and "non-personally identifiable information" (Mot. at 12), but the (s)WAA disclosures use neither of those terms. Again, these terms are also not mutually exclusive. Ex. 42 at 23 (personal information includes "data that can reasonably be linked to" identifying information, including their different Google identifiers). A reference to "non-personally identifiable information" does not expressly notify users that Google will save their (s)WAA-off data, which is what Google needs to unequivocally prove to obtain summary judgment based on its consent defense.

Discovery also revealed that Google intentionally constructed its disclosures to ***avoid*** a clear definition of "Google Account." For example, an employee wrote in June 2016 that "***we're intentionally vague" about data "collected outside of the[] Google Account"*** "because the technical details are complex and it ***could sound alarming to users***." Ex. 1 at -02. The same employee complained that ***the phrase "visible in your Google Account" is "vague about where the data that wasn't visible was."*** *Id.* Google has no right to summary judgment based on disclosures that it made "intentionally vague" to keep users in the dark. Google provides no explanation as to why users would not expect all data associated with their Google identifiers to be "in" their "Google Account," (and thus controlled by the (s)WAA toggle).

Plaintiffs' alternative reading of these disclosures is also supported by their privacy expert, who opines that Google's disclosures contain "dark patterns" (Schneier Rep. § 11), where relevant information is "hid[den], disguise[d], or delay[ed being] divulge[ed]," *Id.* ¶ 311. He discusses how some of Google's disclosures mention the Google Account, others don't, and those that do mention the Google Account omit "the critical fact that even if [users] turn WAA/sWAA off, Google will save data about their online activity outside of their account." *Id.* ¶ 320.[8]

As this Court recognized in its motion to dismiss ruling, the "average internet user is not a full-stack engineer" and "should not be treated as one when Google explains which digital data goes into which digital buckets." Dkt. 109 at 9. Plaintiffs' interpretation does not render anything "surplusage." Mot. at 19. Google assured users that when Google collects users' activity, it is visible in the Google Account portal. Particularly in light of discovery, Google's self-serving interpretation cannot support summary judgment on the issue of consent.

3. General Data-Collection Disclosures Are Insufficient.

Google next leans on general disclosures about its "uses of analytics and ads data." *See* Mot. at 12-14. Google's focus on these general disclosures overlooks well-settled law describing how "consent is not an all-or-nothing proposition." *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1045 (N.D. Cal. 2014). "[C]onsent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct' and if the alleged tortfeasor did not exceed the scope of that consent." *Brown*, 2023 WL 5029899, at *7 (quoting Restatement (Second) of Torts § 892A (1979) §§ 2(b), 4). Google must prove that its disclosures "explicitly notif[ied]" users of the "practice at issue"—here, Google's collection and saving of (s)WAA-off app activity data. *Brown*, 2023 WL 5029899, at *7 (denying motion for summary judgment on express consent).

Brown is instructive. There, Google also sought summary judgment relying on high-level

[8] California banned the use of such dark patterns. *See, e.g.*, Cal. Civ. Code § 1798.140(h), (l).

disclosures about Google's collection of ads and analytics data. *Id.* at *7. The court rejected Google's consent argument, reasoning "there is a dispute as to whether users' consent of Google's data collection generally is 'substantially the same' as their consent to the collection of their private browsing data in particular." *Id.* at *9 (citation omitted). Here, Google points to no disclosure stating it collects ads and analytics data *when (s)WAA is off*. So even if users consented to Google's collection of their app activity data with (s)WAA "on," a juror could still find that users did not consent when (s)WAA was turned "off." *See also Opperman*, 205 F. Supp. 3d at 1076 (denying summary judgment, reasoning even if plaintiffs consented to the defendant "look[ing]" at their phones' contact lists, "permission to look at data does not equate with permission to take it").

Finally, as a variation of its "Google Account" argument, Google now suggests that it should be able to collect whatever data it wants from users' app activity when they have (s)WAA turned off because its claimed practice "is to take significant steps to separate (s)WAA off data from any personally identifiable information belonging to the end user who generated the data." Mot. at 19. No disclosures support this tortured parsing, let alone establish that this is the only reasonable interpretation of Google's disclosures. What is more, courts construe the identifiers at issue here as identifying and "personal information under California law." *In re Google RTB*, 606 F. Supp. 3d at 944 (referring to IP address and "unique device identifier[s]"). California has a "broad definition" of "personal information", *id.*, which includes "unique personal identifier[s], online identifier[s], [and] Internet Protocol address[es]." Cal. Civ. Code § 1798.140(v)(1).

4. Consent Is Disputed for Additional Reasons.

A reasonable juror could alternatively find that Google violated even its own strained and implausible reading of its disclosures. Google's assertion that (s)WAA-off data is not "personal information" conflicts with both reality and the evidence. Google even identifies users by reference to datapoints that Google now claims are "pseudonymous." As explained *supra*, § II.C, including through expert testimony, Google uses device-based identifiers to look up users' (s)WAA settings; maintains linking tables that connect device-based identifiers, app and installation IDs (all unique to individual users) to GAIA; infers (s)WAA-on users' interests from app activity associated with a device-based identifier; and measures and attributes conversions based on device-based identifier. ***There is perhaps no better illustration of Google's ability to connect data collected while (s)WAA was off to individual users' personal identities than what took place in discovery in this very case:*** Plaintiffs requested discovery pertaining to the (s)WAA-off data collected under their names and/or device identifiers and received troves of data tied to the very same. Hochman Rep. ¶¶ 176, 178-80. If that were not enough, there is broad agreement that the information Google collects, such as device identifiers and IP addresses, is "personal information." *See In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d at 944; Cal. Civ. Code § 1798.140(v)(1); 16 C.F.R. § 312.2. A juror could readily agree that (s)WAA-off app activity data is personal information.

Google's summary judgment motion also fails because consent is legally effective only if it is "voluntary." *Hill*, 7 Cal. 4th at 26. In *Hill*, the California Supreme Court taught that consent may be considered "involuntary" if the "consequence" of refusal is exclusion from "a government benefit or an economic necessity that society has decreed must be open to all." *Id.* at 42; *see Hansen v. Cal. Dept. of Corrections*, 920 F. Supp. 1480, 1505 (N.D. Cal. 1996) (holding consent invalid as a matter of law on this basis). Here, Google offers only one way to avoid the challenged privacy violation—abandon the mobile ecosystem altogether. *See* Hochman Rep. ¶¶ 249-51; Ex. 6 at 96:21-97:6, 128:21-129:3 (Google privacy executive is "not aware of any setting" that stops Google's data collection). Class members cannot even prevent Google's data collection by deleting their accounts. *See* Hochman Rep. ¶¶ 249-51. Class members also cannot avoid the non-Google apps where Google collects data: the at-issue Firebase and GMA SDKs are embedded in more than 80% of the most popular apps, and there is no complete list of which ones. *See id.* ¶¶ 2, 59, 355. Even if class members limit themselves to five non-Google apps, they will almost certainly be subject to surveillance. *Id.* ¶ 356 (even if the SDKs' penetration rate were just 50%, there would be a 97% chance of data collection). As this Court pointed out, the only option would be to stop using mobile apps altogether, which "would render Plaintiffs' use of their phones impossible." Dkt. 352 at 13; *see* Hochman Rep. ¶ 1 n.4 (87% of mobile activity occurs on apps). The jury could agree with the Court that mobile devices are "necessities, not luxuries." Dkt. 352 at 13. Under the rule announced in *Hill*, the voluntariness of any consent is disputed at best, non-existent at worst.

B. Triable Issues Also Preclude Summary Judgment on the Privacy Tort Claims.

A rational juror could conclude that "(1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *Facebook Tracking*, 956 F.3d at 601. That juror could also find that Google's conduct is intentional, which is an element only for intrusion upon seclusion. *See Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009) (including this element for intrusion upon seclusion but not invasion of privacy).

1. Objectively Reasonable Expectation of Privacy.

For reasons already explained, a juror could conclude that Google "set an expectation" that when users turn off (s)WAA, their activity on third-party apps "would not be collected." *Facebook Tracking*, 956 F.3d at 602; *see supra* § IV.A. Even under Google's interpretation of its disclosures, a jury would still need to decide whether (s)WAA-off data is "personal information." Leading authorities, expert analysis, and Google's own practices suggest it is. *See supra* § IV.A.4. Google's focus on whether users can expect to "grind the mobile ads ecosystem to a halt" is irrelevant because Plaintiffs' interpretation focuses only on Google's conduct. Mot. at 21.

Courts have rejected Google's argument that people cannot have "a privacy interest in non-personal information." Mot. at 20.[9] "[I]nformation need not be personally identifying to be private." *In re Google Referrer Header*, 465 F. Supp. 3d 999, 1009–10 (N.D. Cal. 2020). In *Brown*, for example, the court ruled at summary judgment that the plaintiffs could have a reasonable expectation of privacy in purportedly anonymous data because "the reason Google has access to their anonymous, aggregated data [was] through the collection and storage of information from users' private browsing history without consent." 2023 WL 5029899, at *5, *19 n.39. In *Wesch v. Yodlee, Inc.*, the court concluded that the plaintiffs could have a "reasonable expectation of privacy in anonymized, aggregated data," because "it would only take a few steps to identify the individual Plaintiffs." 2021 WL 1399291, at *3 (N.D. Cal. Feb. 16, 2021). Here, Plaintiffs are readily identifiable, given Google's association of their (s)WAA-off data to unique Google identifiers.

None of the decisions cited by Google are to the contrary. In *Low v. LinkedIn Corp.*, unlike

[9] This is also not a requirement under the CDAFA, and Google does not contend otherwise.

here, the plaintiff's allegations focused on a portion of LinkedIn's privacy policy that was unambiguously limited to "personally identifiable information." 2011 WL 5509848, at *2, *3 (N.D. Cal. Nov. 11, 2011) (plaintiff failed to allege "what information" was at issue or how one could "infer [his] personal identity" from an "anonymous user ID"); *compare* § II.C (citing detailed evidence that the data is sensitive and identifying). Unlike here, *McCoy v. Alphabet* did not involve data that the defendant promised not to collect. 2021 WL 405816, at *1 (N.D. Cal. Feb. 2, 2021) (plaintiffs were "told Defendant will collect personal data"). The data in *McCoy* also "was not tied to any personally identifiable information, was anonymized, and was aggregated." *Id.* at *8. In this case, Google saves individual (not aggregated) events, and each is associated with unique identifiers that Google will only go so far as to call "pseudonymous" rather than "anonymous" as in the cases it cites. Ex. 6 at 106:23-107:1 (employee admitting that unlike anonymous data, pseudonymous data can be "tied to a data subject"). Even Google's claim that these events are "pseudonymous" is disputed and contravened by the record.

The Ninth Circuit's decision in *Hammerling v. Google LLC*, 2024 WL 937247 (9th Cir. 2024), actually *undermines* Google's Motion. In *Hammerling*, the court found consent because Google *disclosed* that it collects users' "activity on third-party sites and apps that use Google's services." *Id.* at *1 (cleaned up). Here, Google uses *the very same phrase* to describe the data Google will *not* save when (s)WAA is off. *See* Ex. 39 ((s)WAA "[s]aves your *activity on . . . sites, apps, and devices that use Google services*"). For the same reason Google alleged the *Hammerling* plaintiffs consented, Google lacks consent from (s)WAA-off class members.

2. Highly Offensive.

The law "requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Facebook Tracking*, 956 F.3d at 606. "A judge should be cautious before substituting his or her judgment for that of the community." *Opperman*, 205 F. Supp. 3d at 1080.

There is ample evidence that Google's conduct is highly offensive. For example, Google persisted in collecting (s)WAA-off data in spite of concerns raised by its employees. *See Facebook*

Tracking, 956 F.3d at 606 (taking into account that "the company's own officials recognized these practices as a problematic privacy issue"); *Brown*, 2023 WL 5029899, at *20 (denying summary judgment because of "evidence that Google's own employees found the data collection problematic"). Google's "higher-level goal" is not privacy itself but instead "giving users a *sense* of the system working to their benefit." Ex. 70 at -62. Google uses buzzwords like *control* and *choice* to "reassure" and "build trust" with users. Ex. 71 at Row 17. Google even drafted its disclosures to be "intentionally vague" about data "collected outside of the[] Google Account." Ex. 1 at -02. Google's employees think the (s)WAA disclosures are "very deceptive" and predicted that users do not know what "is happening with their data when they disable [(s)WAA]." Ex. 2 at -09; Ex. 41 at -99.R. Studies confirmed that users believe Google does not collect (s)WAA-off data. Ex. 3 at -00, -11. Google's CEO even told Congress that this "toggle" controls "whether" Google collects and stores data. Yet Google made no changes to its practices.

Google's conduct is also highly offensive given the "vast and sensitive" data that it collects while (s)WAA is turned off, and the enormous amount of money it makes using that data. *Brown*, 2023 WL 5029899, at *20; *see supra* § II.C-D. App activity paints an intimate picture of a person's life. *See* Schneier Rep. ¶ 89.[10] As an avalanche of evidence shows, (s)WAA-off app activity data is identifying. *See* §§ II.C, IV.A.4. Plaintiffs will also present evidence of the more than **$664.3 million** in Google profits through 2022. Lasinski Rep. ¶ 129 fig.43. In contrast, Google collects no data through its App Indexing service when (s)WAA is off because that "doesn't add any value" to Google. Ex. 72 at 217:7–15. Profits trump privacy. Class members pay the price: Mr. Lasinski estimates damages equal **$486 million**. Lasinski Rep. ¶¶ 151, 161 fig.50.

Google's cases are far afield. *See Williams v. DDR Media*, 2023 WL 5352896, at *5-7 (N.D. Cal. Aug. 18, 2023) (collection of "minimal" data on a single website, which defendant did "no[t] use"); *Moreno v. S.F. Bay Area Rapid Transit Dist.*, 2017 WL 6387764, at *8 (N.D. Cal. Dec. 14, 2017) (plaintiff was on "notice that [the defendant] would be accessing the information");

[10] *See also*, *FTC Cracks Down on Mass Data Collectors*, FTC (Mar. 4, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/03/ftc-cracks-down-mass-data-collectors-closer-look-avast-x-mode-inmarket.

London v. New Albertson's, Inc., 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) ("plaintiffs concede[d]" that the data was "de-identif[ied]"); *S.F. v. Purdue Pharma L.P.*, 2021 WL 842574, at *2-3 (N.D. Cal. Mar. 5, 2021) (addressing only privilege objections on motion to compel).

3. Intent.

Google represents, without any support, that the required showing of intent is proof that Google "inten[ded] to commit the intentional tort of invasion of privacy." Mot. at 23. That is not the standard. For intrusion upon seclusion, the test is whether Google intended to cause the "consequences of [its] act" or knew those consequences were "substantially certain to result." *Marich v. MGM/UA Telecomms., Inc.*, 113 Cal. App. 4th 415, 421–22 (2003). Substantial evidence proves that Google disseminates its SDKs with knowledge that, as a consequence, Google will collect, save, and use (s)WAA-off data. Exs. 5 at 6, 73 at 4. Evidence also shows that Google knew its users believed Google would not collect (s)WAA-off data. *See supra* § IV.A. At a minimum, there are substantial triable issues of fact on this issue.

C. Material Disputed Facts Concerning Harm and Damage or Loss.

At least five injuries establish common-law harms and "damage or loss" under the CDAFA. Whether Google's conduct has "harmed any class member" (Mot. at 24) is thus disputed.

First, a rational juror could easily find that class members were deprived of their right to privacy, an injury "traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021); *Facebook Tracking*, 956 F.3d at 598 ("Violations of the right to privacy have long been actionable at common law."). What Google calls "basic record-keeping" (Mot. at 1) in fact involves surreptitious and comprehensive collection of class members' activity on apps, which reveals sensitive information about them. *See* Schneier Rep. ¶ 89; *supra* § II.C. Google saves this illicitly acquired data with users' digital fingerprints. This invasion of privacy is legally cognizable harm. *See Campbell*, 951 F.3d at 1117.[11]

[11] Google conflates the concept of harm with the appropriate measure of monetary relief. *See* Mot. at 24-25. All class members suffered injury to their right to privacy. On behalf of the classes, Plaintiffs seek disgorgement of profits, restitution (a form of actual damages), or nominal damages. *See, e.g.*, Restatement (Third) of Restitution § 44 cmt. b ("Profitable interference with . . . [the] right of privacy . . . gives rise to a claim [for restitution and unjust enrichment].").

Second, a rational juror could find that class members suffered damage or loss because Google took their valuable data without permission and then exploited it for profit. *See Facebook Tracking*, 956 F.3d at 600-601 (holding this "establish[es] standing to bring … claims for CDAFA violations"); Lasinski Rep. § 8, ¶¶ 151, 161 (describing this market and value); Ex. 53 at 71:9-73:1, 78:3-80:4, 81:9-82:9 (Plaintiff Cataldo describing value of this data); Ex. 54 at 238:4-240:1, 242:3-21 (Harvey, same); Ex. 55 at 44:19-46:11 (Rodriguez, same); Ex. 52 at 227:8-230:22 (Santiago, same). Google profited at least $664.3 million from (s)WAA-off data. Lasinski Rep. ¶¶ 112, 129 & figs. 34, 43.[12]

Third, a rational juror could find harm or "damage or loss" because "Google failed to pay for collected data despite there being a 'market' for it." Dkt. 352 at 12 n.3; *see Facebook Tracking*, 956 F.3d at 600 (data "carr[ied] financial value" and plaintiffs were uncompensated); *Brown*, 2023 WL 5029899, at *19 (denying summary judgment where "there is a market for [class members'] data"). Here, Google took something that belonged to Plaintiffs, and that something can be valued according to a relevant and reliable measurement of damages "based on the market value" of their mobile data. Dkt. 352 at 20-23; *see also* Lasinski Rep. ¶¶ 132-151 (opining on the market for this data); Ex. 74 at 150:3-156:21 (describing features of the market for mobile data); Ex. 75 at 209:8-14, 242:3-244:24 (recognizing paid "datasharing transaction[s]").

Fourth, a rational juror could find harm or "damage or loss" because Google's collection depletes battery and bandwidth for class members. Dkt. 352 at 12 n.3; *accord In re Carrier IQ*, 78 F. Supp. 3d at 1066-67 (plaintiffs adequately alleged "damage or loss" under the CDAFA based on alleged data collection that "uses system resources, thus slowing performance and decreasing battery life"); *Williams*, 498 F. Supp. 3d at 1200 (recognizing theory of harm based on depletion

[12] This Court already rejected Google's efforts to misrepresent *Facebook Tracking* as bearing only on Article III standing (Dkt. 352 at 11-12), and the dicta in *McClung v. AddShopper, Inc.*, 2024 WL 189006 (N.D. Cal. Jan. 17, 2024), provides no reason to reverse course. Judge Chhabria agreed that *Facebook Tracking* "may … have been intended to convey that the unjust enrichment theory is sufficient to confer statutory standing for claims based on California provisions." *Id.* at n.2. *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1219 (N.D. Cal. 2014), predated *Facebook Tracking* and did not include an analysis of the phrase "damage or loss." And unlike here, those plaintiffs did not allege that there was a market for the data. Lasinski Rep. ¶¶ 132-51.

of device resources). Google's conduct "is an enormous drain on computing resources." Schneier Rep. ¶ 102; Ex. 43 at 138:19-23 (Google "hurts the user by . . . chewing up their mobile device battery and tying up their bandwidth and deteriorating the performance of their device"); Ex. 76 at 224:18-225:7 (data collection "use[s] . . . the end user's device resources and bandwidth"); Ex. 77 at -98 ("pok[ing]" the "connection to a server from a device" can "consume a lot of battery"); Ex. 78 at -10 (Google Analytics affects devices' "battery life").

Fifth, a rational juror could find harm or "damage or loss" because class members did not receive the "benefit of their bargain" with Google. *McClung*, 2024 WL 189006, at *2 (this is "sufficient to confer statutory standing" under the CDAFA). The bargain in this case was that Google would only collect app activity data when (s)WAA is turned on. By violating its promises, Google causes harm—as Google's own expert testified. Ex. 75 at 224:5-21 ("Q: Would you then agree that if Google collects, saves, and uses app activity data from [a (s)WAA-off user], then there is some measure of harm? A: In expected value, directionally speaking, that's correct.").

D. Under the CDAFA, Google Must Obtain Express Permission.

Seeking to escape liability for accessing devices without *class members'* permission, Google relies on permission allegedly given by *third-party app developers*, for whom Google claims to be "agent" and "data processor." Mot. at 25. That is unsupported and unsupportable.

"Ninth Circuit precedent . . . makes clear that [permission] is something that only the owner of the computer or similar authority can provide." *United States v. Thompson*, 2022 WL 834026, at *3 (W.D. Wash. Mar. 21, 2022) (collecting cases). If "authorization to access a computer has been affirmatively revoked," like by turning (s)WAA off, then the defendant "cannot sidestep the statute by going through the back door and accessing the computer through a third party." *United States v. Nosal*, 844 F.3d 1024, 1028 (9th Cir. 2016); *Sols. Team, Inc. v. Oak Street Health, MSO, LLC*, 2018 WL 11432145, at *9 (N.D. Ill. Mar. 5, 2018) ("Even when another party has rights to data stored on a computer, authorization . . . must be provided by the owner ….").[13]

[13] Although *Thompson*, *Nosal*, and *Solutions Team* involved "authorization" under the CFAA, the analysis for "permission" under the CDAFA is "similar" in this regard. *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016) (applying analysis of CFAA claim to CDAFA).

This Court already rejected Google's argument. Moving to dismiss all claims, Google argued that it was "was authorized by . . . the app developers . . . to access and use the information at issue." Dkt. 62 at 19; Dkt. 98 at 24-25. The Court denied Google's motion with respect to the CDAFA claim. *See* Dkt. 109 at 10-12, 14.

Google now relies on a handful of legally and factually inapposite cases to argue that "when a tech company acts as a vendor for another, its scope of consent is coterminous with the party to the communication." Mot. at 25. Other courts have rejected this reasoning. *See, e.g.*, *Valenzuela v. Nationwide Mutual Ins. Co.*, 2023 WL 5266033, at *6-7 (C.D. Cal. Aug. 14, 2023) ("Eavesdropping on a conversation … is a violation … even if done for the benefit of a party to the conversation."). Moreover, these cases concern eavesdropping under the California Invasion of Privacy Act ("CIPA"), not accessing a device under the CDAFA. And even if an app developer could enlist a third party's help to analyze its communications, that does not mean the third party can grant permission to trespass on users' devices and steal data.

Regardless, Google's assertion does not apply here because of two additional disputed facts. First, unlike in any of Google's cases, the plaintiffs here expressly refused to give the defendant permission—they all turned off (s)WAA. Google offered the on or off "choice." Google cannot now "sidestep the statute by going through the back door and accessing the computer through a third party." *Nosal*, 844 F.3d at 1028. Second, unlike in any of Google's cases, there is evidence that Google "intercepted and used the data itself." *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928, 944 (N.D. Cal. 2023) (Seeborg, J.) (distinguishing the cases Google cites). Google does not make money through its work as a "data processor for app developers." Mot. at 25. Google makes money because it also uses (s)WAA-off app activity data for its own purposes: Google uses (s)WAA-off data to serve ads and attribute conversions, ensuring Google's goal of selling ad space to advertisers to arbitrage and collect at a higher price. *See supra* § II.D. And Google uses (s)WAA-off data to improve its own products, including AI, *id.*, and other uses that Google refused to identify, Ex. 51 at 4.

V. CONCLUSION

Google's motion for summary judgment should be denied.

Dated: May 2, 2024

Respectfully submitted,

By: /s/ Mark C. Mao

Mark C. Mao (CA Bar No. 236165)
mmao@bsfllp.com
Beko Reblitz-Richardson (CA Bar No. 238027)
brichardson@bsfllp.com
BOIES SCHILLER FLEXNER LLP
44 Montgomery Street, 41st Floor
San Francisco, CA 94104
Telephone: (415) 293 6858
Facsimile (415) 999 9695

David Boies (admitted *pro hac vice*)
dboies@bsfllp.com
BOIES SCHILLER FLEXNER LLP
333 Main Street
Armonk, NY 10504
Telephone: (914) 749-8200

James Lee (admitted *pro hac vice*)
jlee@bsfllp.com
Rossana Baeza (admitted *pro hac vice*)
rbaeza@bsfllp.com
BOIES SCHILLER FLEXNER LLP
100 SE 2nd Street, Suite 2800
Miami, FL 33131
Telephone: (305) 539-8400
Facsimile: (305) 539-1307

Alison L. Anderson, CA Bar No. 275334
alanderson@bsfllp.com
M. Logan Wright, CA Bar No. 349004
mwright@bsfllp.com
BOIES SCHILLER FLEXNER LLP
2029 Century Park East, Suite 1520
Los Angeles, CA 90067
Telephone: (813) 482-4814

Bill Carmody (*pro hac vice*)
bcarmody@susmangodfrey.com
Shawn J. Rabin (*pro hac vice*)
srabin@susmangodfrey.com
Steven Shepard (*pro hac vice*)
sshepard@susmangodfrey.com

Alexander P. Frawley
afrawley@susmangodfrey.com
Ryan Sila
rsila@susmangodfrey.com
SUSMAN GODFREY L.L.P.
One Manhattan West, 50th Floor
New York, NY 10001
Telephone: (212) 336-8330

Amanda Bonn (CA Bar No. 270891)
abonn@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Telephone: (310) 789-3100

John A. Yanchunis (*pro hac vice*)
jyanchunis@forthepeople.com
Ryan J. McGee (*pro hac vice*)
rmcgee@forthepeople.com
Michael F. Ram (CA Bar No. 238027)
mram@forthepeople.com
MORGAN & MORGAN, P.A.
201 N Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 222-4736

Attorneys for Plaintiffs